

88



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/882,374	06/12/2001	Tia Walker	32628-8001US2	6743

25096 7590 02/28/2005

PERKINS COIE LLP  
PATENT-SEA  
P.O. BOX 1247  
SEATTLE, WA 98111-1247

EXAMINER

TRAN, ELLEN C

ART UNIT	PAPER NUMBER
----------	--------------

2134

DATE MAILED: 02/28/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

**Office Action Summary**

Application No.

09/882,374

Applicant(s)

WALKER ET AL.

Examiner

Ellen C Tran

Art Unit

2134

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --  
**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 12 June 2001.
- 2a) ☐ This action is **FINAL**.                      2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1-49 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-49 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 10 October 2001 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All    b) ☐ Some \*    c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- \* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)  
Paper No(s)/Mail Date \_\_\_\_\_.
- 4) ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date. \_\_\_\_\_.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: \_\_\_\_\_.

**DETAILED ACTION**

1. This action is responsive to communication: original application filed 12 June 2001, with acknowledgement of continuing filing date of 12 June 2000.
2. Claims 1-49 are currently pending in this application. Claims 1, 16, 28, and 38 are independent claims.

***Claim Rejections - 35 USC § 102***

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language

4. **Claims 1-11, 13, 16-41 and 43-49** are rejected under 35 U.S.C. 102(e) as being anticipated by Liu et al. U.S. Patent No. 6,760,752 (hereinafter '752).

**As to independent claim 1, "A method in a client computer for encrypting an electronic mail message, the method comprising:"** is taught in '752 col. 1, lines 54-65;

**"receiving an indication to encrypt the electronic mail message, the electronic mail message having a recipient electronic mail address" and "a public key associated with the recipient electronic mail address"** is shown in '752 col. 16, lines 4-44;

**"retrieving from a local key store"** is disclosed in '752 col. 3, lines 12-18;

**"when the public key cannot be retrieved from the local key store, retrieving from a key server the public key associated with the recipient electronic mail address"** is taught in '752 col. 13, lines 12-54;

**“and encrypting the electronic mail message using the retrieved public key” is shown in ‘752 col. 1, lines 54-65.**

**As to dependent claim 2, “including sending the encrypted electronic mail message to the recipient electronic mail address” is disclosed in ‘752 col. 16, lines 4-44.**

**As to dependent claim 3, “wherein the retrieving from the key server includes: sending to the key server a request for the public key associated with the recipient electronic mail address; and receiving from the key server a response including the public key associated with the recipient electronic mail address” is shown in ‘752 col. 16, lines 4-44.**

**As to dependent claim 4, “wherein when the key server does not already have a public key associated with the recipient electronic mail address, the key server associates a new public and private key pair with the recipient electronic mail address” is disclosed in ‘752 col. 12, lines 40-67.**

**As to dependent claim 5, “wherein the key server sends a notification electronic mail message to the recipient electronic mail address describing how to access the new private key associated with the recipient electronic mail message” is taught in ‘752 col. 13, line 38 through col. 14, line 43.**

**As to dependent claim 6, “wherein the notification electronic mail message includes an authentication code so that a user accessing the new private key can be authenticated by presentment of the authentication code” is shown in ‘752 col. 2, lines 41-45.**

As to dependent claim 7, “wherein the notification electronic mail message includes a link to a web site through which the new private key can be accessed” is disclosed in ‘752 col. 21, lines 21-37.

As to dependent claim 8, “wherein the new private key is an interim key” is taught in ‘752 col. 8, line 60 through col. 9, line 18 and col. 2, lines 62-67.

As to dependent claim 9, “including storing the public key retrieved from the key server in the local key store” is disclosed in ‘752 col. 7, lines 4-21 and col. 3, lines 12-16.

As to dependent claim 10, “wherein when the public key retrieved from the key server is an interim key, suppressing the storing of the public key in the local key store” is taught in ‘752 col. 21, lines 20-52.

As to dependent claim 11, “including sending to the key server a request for the public key associated with the recipient electronic mail address; receiving from the key server a response indicating that no public key is associated with the recipient electronic mail address; and in response to receiving the response, sending to the key server a request that a public and private key pair be associated with the recipient electronic mail address; and receiving from the key server a response including the public key newly associated with the recipient electronic mail address” is taught in ‘752 col. 12, lines 40-67.

As to dependent claim 13, “including signing the electronic mail message with a private key associated with a sender of the electronic mail message” is shown in ‘752 col. 1, lines 54-60.

**As to independent claim 16, “A method in a server computer for coordinating sending of an electronic mail message from a sender to a recipient, the method comprising” is taught in ‘752 col. 1, lines 54-65;**

**“receiving from a sender computer a request for a public key associated with a recipient electronic mail address; associating a public and private key pair with the recipient electronic mail address; sending to the sender computer a response that includes the public key associated with the recipient electronic mail address; and providing the private key to the recipient so that the electronic mail message encrypted by the sender using the public key can be decrypted by the recipient using the private key” is shown in ‘752 col. 16, lines 4-44;**

**As to dependent claim 17, “wherein the providing of the public key to the recipient includes sending a notification electronic mail message to the recipient electronic mail address” is disclosed in ‘752 col. 16, lines 4-44.**

**As to dependent claim 18, “wherein the notification electronic mail message includes an authentication code that is used to authenticate the recipient” is taught in ‘752 col. 17, lines 63 through col. 18, line 13;**

**“when the interim private key is provided to the recipient” is shown in ‘752 col. 8, line 60 through col. 9, line 18 and col. 2, lines 62-67.**

**As to dependent claim 19, “wherein the notification electronic mail message includes the private key” is taught in ‘752 col. 13, line 38 through col. 14, line 43.**

**As to dependent claim 20, “including when a subsequent request is received from a sender computer for a public key associated with the recipient electronic mail address,**

**sending to the sender computer the public key previously associated with the recipient electronic mail address” is shown in ‘752 col. 16, lines 4-44 and col. 13, lines 12-54.**

**As to dependent claim 21, “wherein the public key is an interim key” is disclosed in ‘752 col. 2, lines 61-67;**

**“and the sender computer does not persistently store the interim public key” is taught in ‘752 col. 3, lines 17-25.**

**As to dependent claim 22, “wherein the public and private key pair is used as a permanent public and private key pair for the recipient” is shown in ‘752 col. 7, lines 4-36.**

**As to dependent claim 23, “wherein the public and private pair is used as a permanent public and private key pair for the recipient when requested by to do so by the recipient” is disclosed in ‘752 col. 21 line 20 through col. 22, line 67.**

**As to dependent claim 24, “including receiving a permanent public key from the recipient and replacing the public key with the received permanent public key” is taught in ‘752 col. 21 line 20 through col. 22, line 67.**

**As to dependent claim 25, “including generating the public and private key pair” is shown in ‘752 col. 21 line 20 through col. 22, line 67.**

**As to dependent claim 26, “including selecting the public and private key pair from a pool of previously generated public and private key pairs” is disclosed in ‘752 col. 21 line 20 through col. 22, line 67.**

**As to dependent claim 27, “including changing an electronic mail address associated with the selected public and private key pair to the recipient electronic mail address” is taught in ‘752 col. 25, lines 1-67.**

**As to independent claim 28, “A method in a server computer for coordinating sending of an electronic mail message from a sender to a recipient, the method comprising”** is taught in ‘752 col. 1, lines 54-65;

**“receiving from a sender computer a request to send the electronic mail message to a recipient electronic mail address; encrypting the electronic mail message with a public key associated with the recipient; sending the encrypted electronic mail message to the recipient electronic mail address; and sending a private key to the recipient so that the electronic mail message can be decrypted by the recipient using the sent private key”** is shown in ‘752 col. 16, lines 4-44.

**As to dependent claim 29, “wherein the sending of the private key to the recipient includes sending of a notification electronic mail message to the recipient electronic mail address”** is shown in ‘752 col. 16, lines 4-44.

**As to dependent claim 30, “wherein the notification electronic mail message includes an authentication code that is used to authenticate the recipient before sending the private key”** is shown in ‘752 col. 2, lines 41-45.

**As to dependent claim 31, “wherein the notification electronic mail message includes the private key”** is taught in ‘752 col. 13, line 38 through col. 14, line 43.

**As to dependent claims 32-37**, these claims contain substantially similar subject matter as claims 22-27 and are rejected along the same rationale.

**As to independent claim 38, “A method in a client computer for encrypting digital data, the method comprising:”** is taught in ‘752 col. 1, lines 54-65;



**“receiving an indication to encrypt digital data; and “a locking key associated with a user; when the locking key cannot be retrieved from the local key store, retrieving from a key server the locking key associated with the user; and encrypting the digital data using the retrieved locking key”** is shown in ‘752 col. 16, lines 4-44.

**“retrieving from a local key store”** is disclosed in ‘752 col. 3, lines 12-18.

**As to dependent claim 39, “wherein the user has a user identifier and the locking key is mapped to the user identifier”** is taught in ‘752 col. 2, lines 22-39.

**As to dependent claim 40, “wherein the user identifier is an electronic mail address”** is disclosed in ‘752 col. 2, lines 22-39.

**As to dependent claim 41, “wherein the user identifier is a key identifier associated with the locking key”** is taught in ‘752 col. 2, lines 22-36.

**As to dependent claim 43, “wherein the encrypted digital data is decrypted using an unlocking key”** is shown in ‘752 col. 15, lines 30-42.

**As to dependent claim 44, “wherein the locking key is a public key of a public and private key pair”** is disclosed in ‘752 col. 15, lines 30-42.

**As to dependent claim 45, “wherein the digital data is content of a file”** is taught in ‘752 col. 15, lines 30-42.

**As to dependent claim 46, “wherein the digital data is content of an electronic mail message”** is shown in ‘752 col. 15, lines 30-42.

**As to dependent claim 47, “wherein the key server receives a request for a locking key for the user, it assigns a locking and unlocking key pair to the user and provides the unlocking key to the user”** is disclosed in ‘752 col. 16, lines 4-44.

As to dependent claim 48, “wherein the key server notifies the user that a locking and unlocking key pair has been assigned to the user before providing the unlocking key to the user” is shown in ‘752 col. 23, lines 7-64.

As to dependent claim 49, “wherein the key server provides an authentication code for authenticating the user” is disclosed in ‘752 col. 2, lines 41-45.

***Claim Rejections - 35 USC § 103***

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

6. **Claim 12** is rejected under 35 U.S.C. 103(a) as being unpatentable over ‘752 in further view of Smith et al. U.S. Patent No. 6,651,166 (hereinafter ‘166).

As to dependent claim 12, the following is not taught in ‘752 “wherein the electronic mail message is to be sent by a sender and including logging the sender on to the key server” however ‘166 teaches “The client 70 can then “click” or access this URL through a standard web browser. Accessing the URL begins a direct interaction or SDCE conversation 68, between the client 70 and the SDCE server 58” in col. 5, lines 15-45.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify a method of sending encrypted emails taught in ‘752 to include a means to for the sender to log into a key server. One of ordinary skill in the art would have been motivated to perform such a modification to because of the challenges faced with key distribution methods see ‘166 col. 4, lines 37 et seq. “One potential issue with secret key encryption 10a and 10b is

the challenge of distributing the secret key 14 securely ... In some instances, however, senders and recipients require a more robust or convenient means of distributing a secret key”.

7. **Claims 14, 15, and 42** are rejected under 35 U.S.C. 103(a) as being unpatentable over ‘752 in further view of Haff et al. U.S. Patent No. 6,442,571 (hereinafter ‘571).

**As to dependent claim 14**, the following is not taught in ‘752 **“wherein the encrypted electronic mail message is received at the recipient electronic mail address, the encrypted electronic mail message is automatically decrypted using a private key associated with the recipient electronic mail address”** however ‘571 teaches “Files received at a PC destination that were encrypted using the public key for that destination are decrypted automatically using the private key for the receiving PC” in col. 36 line 59 through col. 37, line 13.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify a method of sending encrypted emails taught in ‘752 to include a means to further limit the control of encryption and decryption of electronic mail received. One of ordinary skill in the art would have been motivated to perform such a modification because a file transfer system is needed that is not limited by the shortcoming of the prior art see ‘571 col. 2, lines 31 et seq. “The approaches, as embodied in the physical and the electronic document delivery systems in use today, exhibit a number of shortcomings... Further, these intermediary computers represent concentrated points of possible failure, as well as communication “bottlenecks” that set capacity limits for the collective number and size of files transferred”.

**As to dependent claim 15**, **“wherein when a recipient receives the encrypted electronic mail message, the decrypting of the received electronic mail message is deferred until a request to decrypt is received”** is taught in ‘571 col. 46, line 50 through col. 47, line 3

Art Unit: 2134

“Received files can be decrypted using the recipients private key if public key encryption is implemented. Alternatively, received files can be automatically decrypted if one-time-pad encryption is implemented and the recipient's identity and decryption request to the security server comply with implemented security policy. Various security service policies, such as station to station encryption or person to person encryption can be effected”.

**As to dependent claim 42, “wherein the user identifier is a user name”** is shown in ‘571 col. 32, lines 31-44 “In a preferred embodiment, text identifying the user's name, organization, and address are automatically inserted”.

***Conclusion***

8. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Al-Salqan                      U.S. Patent No. 6,775,382                      issued 10 Aug 2004

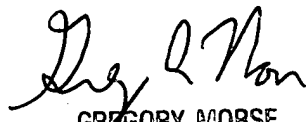
Vanstone et al.              U.S. Patent No. 6,446,207                      issued 3 Sept 2002

9. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ellen C Tran whose telephone number is (571) 272-3842. The examiner can normally be reached from 6:30 am to 3:30 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory A Morse can be reached on (571) 272-3838. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Ellen Tran  
Patent Examiner  
Technology Center 2134  
4 February 2005

  
GREGORY MORSE  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2134